High-Availability User Networks

0490 By extension of the PBSN concept, using the Data Replication Agent software element, a computer user can have, invisibly, multiple local and remote copies of the all of the user's important data made on the PBSN (see Figure 15). By this means, any user that suffers a computer failure can access data immediately through any other computer on the PBSN. This method can be extended to encompass a full image of the user's working data, so that building a new computer can be accomplished in a very short time by simply copying that image from the PBSN to the new computer. These features are a part of the PBSN agent's Data Replication Agent function.

0500 Since the DEA system uses very long encryption keys, which are not memorisable, to provide the encryption capability, it is necessary to provide a means to store these keys in case of the failure of a user's computer. A number of methods are available to achieve this, ranging from physical keys such as security cards, smart cards or keys or even microchips embedded under the skin, to logical access systems using passwords or lookup files, among other means. Several of these means have some level of security exposure. The DEA and the other software elements of the invention are designed to support a variety of these means, allowing for different levels of security in the installed product.

Alternative Implementations of the Invention

0510 An alternative method (Figure 16) of building the SNAS system is to install the DAC, the ARD and some of the other software facilities on a network switching device, such as a SAN, LAN or Wide Area Network switch, hub or router; so effectively making the redirections within that switching device and effectively invisible in most circumstances to the client computers.